State of Colorado
Cyber Security Policies

Incident Response

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document.

For the purposes of this document, an "Agency" includes organizations as defined in C.R.S 24-37.5-102(5).

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403, C.R.S. 24-37.5-404(2)(e), C.R.S. 24-37.5-405.

Policy

The State of Colorado has established a Cyber Security Incident Response Plan (CSIRP) to effectively address the need for the successful handling of and proper response to computer security incidents. All computer security incidents must be reported in accordance with policies and procedures established in this document. The primary purpose of the CSIRP is to protect and maintain current operations that support the mission of the State of Colorado and its various agencies.

The State shall maintain a Cyber Security Incident Response Team (CSIRT) that reports directly to the Chief Information Security officer (CISO) and shall maintain a plan to effectively guide response to a cyber incident.

Scope

This policy applies to all State agencies as defined in C.R.S. 24-37.5-102(5)**.** State-supported institutions of higher education, the department of higher education, the Colorado commission on higher education and other instrumentality thereof (collectively referred to as "Higher Education" throughout this policy) must comply with this policy in a limited context as described in the Requirements section.

Definitions

For the purposes of this document, refer to C.R.S. 24-37.5-102, C.R.S 24-37.5-402, and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

State CISO – is responsible for:

- Activating the Cyber Security Incident Response Team (CSIRT).
- Providing executive decisions required by the Cyber Security Incident Response Team.

Cyber Security Incident Response Coordinator – is responsible for leading and managing the Incident Response Team.

Agency Information Security Officer (ISO) – is responsible for developing and implementing localized agency-level procedures for incident reporting.

Higher Education – is responsible for developing and implementing an Incident Response Plan according to the requirements of this document and supporting it with localized institution procedures for incident response and reporting.

Requirements

All agencies must appoint an Information Security Officer that participates on this multi-agency team and develops localized agency-level procedures for incident monitoring, responding and reporting in accordance with the Colorado Incident Response Plan and associated Quick Reference Guides where applicable.

Higher Education must develop an Incident Response Plan and submit the plan to the CISO for review and comment. The Higher Education Plan must identify the reporting relationships between Higher Education and the CISO, to include defining the stage during an Incident Response at which incidents are reported to the Information Security Operations Center (ISOC) and CISO, explaining the role of the ISOC and CISO in the plan, and containing a periodic metric reporting requirement to the CISO.

Guidelines

See the Colorado Incident Response Plan for details.

References

- Colorado Incident Response Plan
- Colorado Incident Response Quick Reference Guides